

12

DEMANDE DE BREVET EUROPEEN

21 Numéro de dépôt: 87450009.3

51 Int. Cl.³: **E 05 B 49/00**

22 Date de dépôt: 16.04.87

30 Priorité: 22.04.86 FR 8606217

43 Date de publication de la demande:
04.11.87 Bulletin 87/45

84 Etats contractants désignés:
CH DE ES GB IT LI SE

71 Demandeur: Soum, René
33 Rue Montcabrier
F-31500 Toulouse(FR)

72 Inventeur: Soum, René
33 Rue Montcabrier
F-31500 Toulouse(FR)

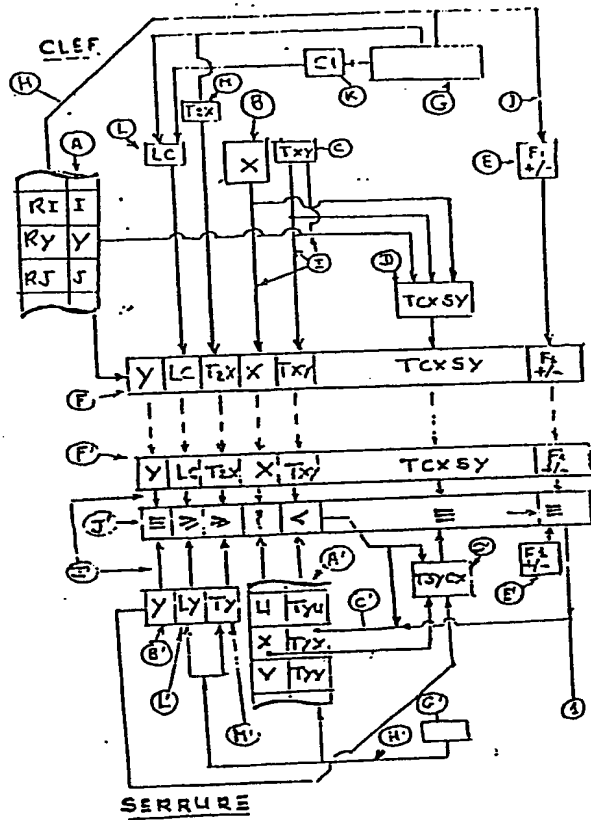
74 Mandataire: Ravina, Bernard
Cabinet Bernard RAVINA 24, boulevard Riquet
F-31000 Toulouse(FR)

54 **Système de très haute sécurité de télécommande sans fil permettant l'ouverture ou la fermeture inviolable de relais actionnant des systèmes tels que serrures.**

57 Le système selon l'invention comprend un ensemble de clés (X) et serrures de sécurité (Y) à télécommande dans lequel la clé n'a qu'une fonction d'émission et la serrure de réception associant aux fonctions de sécurité absolue d'ouverture ou de fermeture des serrures, celle d'antivol clés par paramétrisation des serrures.

EP 0 244 332 A1

./...



SYSTEME DE TRES HAUTE SECURITE DE TELECOMMANDE SANS FIL PERMETTANT L'OUVERTURE OU LA FERMETURE INVIOLEBLE DE RELAIS ACTIONNANT DES SYSTEMES TELS QUE SERRURES.

La présente invention concerne un système de très haute sécurité de télécommande sans fil, permettant l'ouverture ou la fermeture inviolable de relais actionnant des systèmes tels que serrures et l'association de ce système :

- à une fonction antivol de la clé, à des conditions de sécurité choisies par l'utilisateur et imposées à la serrure.

Les systèmes actuels à télécommande permettent la reconnaissance d'un code transmis par une clé vers une serrure, et d'actionner cette dernière.

Mais ils présentent l'inconvénient majeur de permettre l'interception des codes émis par la clé et leur reproduction et sont, de ce fait, d'une sécurité discutable.

Des systèmes à N codes multiples pré-enregistrés, successivement émis à partir d'un compteur et d'une table, le dit compteur étant remis à zéro périodiquement, ont été proposés mais les messages ainsi émis sont périodiquement réémis et sont donc interceptables et ils exigent une parfaite transmission de l'émetteur vers le récepteur afin d'éviter le décalage des compteurs entre eux.

Des systèmes surs utilisent dans chaque clé et serrure un émetteur et un récepteur et sont, de ce fait, onéreux.

La présente invention n'utilise qu'une fonction d'émission pour la clé et de réception pour la serrure.

Elle interdit toute utilisation des messages interceptés lors d'une manoeuvre, car tout message ayant servi une fois à action-

ner une serrure, ne pourra être utilisé une nouvelle fois pour actionner cette dernière.

Elle ajoute à ces avantages les fonctions supplémentaires ci-avant évoquées, toujours en n'utilisant que les fonctions d'émission par la clé et de réception par la serrure, et complète en un seul élément les dispositifs de commande avec un dispositif anti-vol n'autorisant l'usage de la clé que sous les conditions imposées avant chaque manoeuvre, par la propriétaire de la serrure, maître du niveau de sécurité d'utilisation des couples clé-serrure.

Le système clé-serrure, objet de l'invention, comporte une clé numéro X comprenant :

- une mémoire "A" des repères Ry des serrures à actionner, associées aux numéros Y de ces serrures.

Ry et Y sont introduits dans la clé par son utilisateur et mémorisés dans "A" une fois pour toutes.

Le repère Ry de la clé, librement choisi par son utilisateur, est unique pour chaque clé qui l'associe à Y, numéro de la serrure, dans une table de correspondance.

Une serrure sera désignée au clavier de la clé par son repère, lequel repère peut, si l'utilisateur le désire, être identique au numéro de la clé.

La mémoire "A" comporte donc la liste de tous les duos Ry, Y des serrures à actionner.

- Une mémoire "B" du numéro X de la clé considérée.

A chaque clé correspond un numéro X unique, inscrit dans "B" par construction de la clé.

- Un compteur interne à la clé avec sa mémoire "C" qui s'incrémente d'une façon univoque à chaque manoeuvre de la clé d'une valeur quelconque permettant de vérifier l'incrémentation univoque de l'état T, X, Y du compteur de la clé.
- Un calculateur "D" combinant, par un algorithme irréversible à clé secrète, le numéro Y de la serrure repéré par le repère Ry de la serrure que l'on désire actionner, avec d'une part le numéro X de la clé, et d'autre part, l'état T, X, Y du compteur à incrémentation univoque, variable, la dite combinaison T C X S Y, obtenue et transmise à la serrure, variant donc à chaque utilisation de la clé.
- Une mémoire "E" comportant par construction de la clé deux signaux Fl+ et Fl-, chacun de ces signaux reconnaissables par la serrure, signifiant à cette dernière le type d'ordre reçu, ouverture ou fermeture.
- Un émetteur "F" transmettant à la serrure par tous moyens connus le numéro Y de la serrure à actionner, le numéro X de la clé en action, l'état T X Y du compteur interne, le résultat T C X S Y de la combinaison des numéros X et Y de la serrure et de la clé avec T X Y.
Y, X, T X Y et T C X S Y, émis et interceptables, ne sont pas secrets.
T X Y et T C X S Y changent lors de chaque émission.
Seule la clé numéro X peut générer T C X S Y car X est unique et l'algorithme de génération de T C X S Y est secret.
- Des moyens "G" d'introduction des Ry, Y dans "A" et de repérage

de la serrure concernée dans "A" par Ry, avec les liaisons "H" correspondantes, les liaisons "I" de "A", "B" et "C" avec "D", et de commande de "C".

Le système clé-serrure, objet de l'invention, comporte une serrure comprenant :

- une mémoire "A" des numéros X des clés autorisées à l'actionner, associés à l'état T Y X du compteur interne de chaque clé reçu lors de la dernière action de chaque clé sur la serrure. Les numéros des clés sont introduits dans la serrure par son utilisation et mémorisés dans "A".
- Une mémoire "B" du numéro Y de la serrure, mémorisé dans la serrure par construction. A chaque serrure correspond par construction un numéro Y unique.
- Une liaison "C" incrémentant au niveau T X Y émis par la clé, l'état du compteur serrure de chaque T Y X relatif à chaque clé X, lors de chaque manoeuvre effective de la serrure Y par la clé X, les numéros X et Y étant émis par la clé, et reçus par la serrure avec l'état T X Y du compteur clé.
- Un calculateur "D" identique, à celui de la clé combinant par un algorithme irréversible à clé secrète, le numéro Y de la serrure avec, d'une part, le numéro X de la clé reçu lors de l'émission de cette dernière, et d'autre part, l'état du compteur interne T X Y reçu de la clé, après que la serrure ait vérifié que T X Y est à un niveau incrémenté par rapport à l'état antérieur à l'action de la clé, T Y X mémorisé dans "A".

- Une mémoire "E" comprenant par construction de la serrure deux signaux Fl+ et Fl-, les dits signaux identiques à ceux de la clé et signifiant à la serrure par comparaison, le type d'ordre reçu, ouverture ou fermeture.
- Un récepteur "F" recevant de la clé les informations émises par cette dernière.
- Des moyens "G" d'introduction des X dans "A" et les liaisons "H" correspondantes, les liaisons "I" de "A", "B" et "F" avec "D", de commande "C", et de liaison avec le comparateur "J".
- Un comparateur "J" vérifiant que le numéro Y reçu de la clé correspond bien au numéro Y de la serrure, que le numéro X de la clé est bien mémorisé dans la serrure, que l'état du compteur T X Y reçu de la clé est bien à un niveau supérieur à l'état T Y X mémorisé dans la mémoire "A" du message précédent correspondant reçu de la clé, que la combinaison T C X S Y reçue de la clé est identique à la combinaison T S Y C X déterminée par la serrure, le dit comparateur autorisant l'action Fl+ ou Fl- selon le signal reçu de la clé, si toutes les conditions précédentes sont réunies et incrémentant le dit compteur T Y X de la serrure au niveau T X Y du compteur clé.

L'ensemble clé-serrure de l'invention répond à toutes les sécurités exigées en la matière.

La clé ne peut actionner la serrure que si l'on a enregistré dans sa mémoire le numéro Y de la serrure, et la serrure ne peut être actionnée par la clé que si l'on a enregistré dans sa

mémoire le numéro X de la clé.

Ces introductions sont protégées par un code d'accès à la mémoire de chacun des éléments.

Afin que les messages émis par la clé ne puissent être utilisés s'ils sont interceptés, ils comprennent la combinaison des numéros serrure et clé avec l'état d'un compteur interne à incrémentation univoque, la serrure vérifiant avant d'accepter le message, que ce compteur a été incrémenté d'une part, et d'autre part, que les numéros des serrures sont corrects et que la combinaison générée par la serrure après l'incrémentation du compteur interne de cette dernière au niveau de celui émis par la clé, combinaison variable à chaque émission en raison de l'incrémentation des compteurs clé et serrure, donc non susceptible d'actionner une nouvelle fois la serrure si elle est reproduite.

Les moyens informatiques connus permettent d'empêcher la lecture dans la mémoire de la clé ou de la serrure, des informations qui y sont inscrites par construction ou par écriture, en particulier de l'algorithme, la possession temporaire de la clé ou de la serrure, par un fraudeur n'autorisant pas, de ce fait, la génération ultérieure de messages corrects en l'absence de la possession de la clé.

L'invention assure donc toute sécurité de fonctionnement sur la base d'un émetteur formant clé et d'un récepteur formant serrure, cette dernière actionnant les relais électromécaniques "1" d'ouverture et de fermeture.

Les ensembles clé-serrure ainsi constitués sont inviolables ; ils permettent à un ensemble de clés d'ouvrir une serrure par intro-

duction dans chaque clé des informations serrure, et dans la serrure des informations clé, et à chaque clé d'ouvrir un ensemble de serrures par la même méthode.

Toutes combinaisons de passe-partout sont ainsi possibles.

L'interception des messages ne permet en aucun cas, même s'ils sont reproduits, d'actionner la serrure ou de perturber son fonctionnement car l'état T Y X du compteur serrure, miroir du compteur clé, n'est mis au niveau T X Y du compteur de la clé que si la serrure a été effectivement actionnée.

L'utilisation d'un algorithme secret à clé partiellement secrète pour la génération de T C X S Y, message d'ouverture, le dit algorithme étant inscrit d'une façon non lisible dans le calculateur, ne permet en aucun cas de générer un T C X S Y correct si l'on n'est pas possesseur de la clé, car le numéro de la clé est unique et l'algorithme secret.

Enfin, l'irréversibilité de l'algorithme ne permet pas de déterminer les futurs messages d'ouverture à partir des messages successifs reçus de la clé, même si ces derniers sont interceptés.

La fonction ouverture-fermeture des ensembles clé-serrures associe la télécommande à une inviolabilité absolue et répond au but proposé.

Afin qu'un fraudeur s'emparant de la clé ne puisse l'utiliser, cette dernière comporte une sécurité d'utilisation : chaque serrure impose qu'un certain nombre LC de caractères d'un code C1, le dit nombre choisi par le propriétaire de la serrure, et le dit code C1 choisi par l'utilisateur de la clé, ait été introduit dans la clé depuis un temps inférieur à un délai maximum TY imposé par la serrure, avant toute manoeuvre.

Pour réaliser ce système, la clé comporte une mémoire "K" de ce code C1 choisi par l'utilisateur, un comparateur L donnant le nombre Lc de caractères, identiques à ceux du code C1 introduits dans la clé, une horloge "M" donnant le temps T2x depuis lequel cette portion de code a été introduite.

Les signaux LC et T2x sont émis par "F" et reçus par "F'" dans la serrure.

La serrure comporte une mémoire "L'" du nombre Ly de caractères minimum imposés et une mémoire "M'" du délai maximum Ty imposé par la clé depuis l'introduction du code dans la clé.

La serrure comporte un comparateur "J'" comparant la longueur Lc du code émis par la clé à la longueur minimale Ly imposée, et le délai T2x donné par la clé au délai maximum Ty accordé par la serrure, la dite serrure interdisant toute manoeuvre si Ly ou T2x sont respectivement supérieurs à Lc et Ty.

Ce dispositif permet le contrôle par la serrure de l'utilisation d'un code d'une longueur minimale dans la clé dans un certain délai, sans que ce code soit émis vers la serrure neutralisant ainsi toute tentative d'interception de ce code lors des émissions et assurant la sécurité d'utilisation de la clé par la serrure.

Cette sécurité supplémentaire interdit l'utilisation de la clé par un fraudeur en laissant à l'utilisateur le choix du niveau de la sécurité choisi introduit dans la serrure.

L'invention proposée assure la totale inviolabilité du système clés-serrures à télécommande, car d'une part, la combinaison émise variable à chaque manoeuvre, est à la fois imprévisible, inef-

ficace si elle est reproduite, particulière à chaque clé et d'autre fpart, en cas de perte de la clé, un système d'autorisation par code neutralise l'utilisation de la clé par un fraudeur, la dite interdiction étant contrôlée par la serrure.

REVENDEICATIONS :

1. Ensemble de clés et serrures de sécurité à télécommande dans lequel la clé n'a qu'une fonction d'émission et la serrure de réception associant aux fonctions de sécurité absolue d'ouverture ou fermeture des serrures, celle d'antivol clé par paramétrisation des serrures, caractérisé en ce qu'il associe dans la clé des mémoires où sont enregistrés les signaux représentant le numéro de la clé et les numéros des serrures à actionner à un signal représentant l'état d'un compteur interne à mémoire incrémenté d'une façon univoque à chaque action sur la clé, la valeur représentant le dit compteur ayant à chaque action de la clé une valeur incrémentée différente de toutes ses valeurs antérieures.

2. Système selon la revendication 1 caractérisé en ce qu'il comporte dans la serrure des mémoires où sont enregistrés les signaux représentant les numéros des clés autorisées à actionner la serrure, le numéro de la serrure, les dites mémoires étant associées à la mémoire de l'état du signal transmis par chaque clé représentant l'état du compteur interne de la clé à incrémentation univoque lors de la dernière manoeuvre effectuée par cette clé sur la serrure et acceptée par cette dernière.

3. Système selon les revendications 1 et 2 caractérisé en ce que la clé transmet à la serrure les signaux représentant son numéro, le numéro de la serrure à actionner et l'état du compteur interne de la clé à incrémentation univoque.

4. Système selon les revendications 1, 2 et 3 caractérisé en ce que le numéro de chaque clé et de chaque serrure est unique et attribué par construction.

5. Système selon les revendications 1 à 4 prises dans leur ensemble, caractérisé en ce que la clé comporte un calculateur algorithmique générant, par combinaison des signaux représentant le numéro de la serrure et de la clé avec le signal représentant l'état variable de son compteur interne à incrémentation univoque, des signaux représentant des messages d'ouverture ou fermeture successifs, variables à chaque action de la clé et imprévisibles, émis par la clé.

6. Système selon les revendications 1 à 5 prises dans leur ensemble, caractérisé en ce que la serrure comporte un comparateur vérifiant que le signal représentant l'état du compteur interne à incrémentation univoque reçu de la clé, est à un niveau supérieur à celui du signal représentant l'état du compteur interne à incrémentation univoque mémorisé dans la serrure lors de la précédente manoeuvre effectuée et interdisant de ce fait, l'ouverture de la serrure par reproduction d'un précédent message d'ouverture.

7. Système selon les revendications 1 à 6 prises dans leur ensemble, caractérisé en ce que la serrure comporte un calculateur identique à celui de la clé générant un signal à partir des données de la serrure et de la clé et de l'état vérifié du signal représentant le compteur à incrémentation univoque de la clé, le dit signal comparé dans un comparateur autorisant la manoeuvre ordonnée par la clé s'il y a identité des signaux émis

par la clé et généré par la serrure constituant un message d'ouverture ou fermeture variable à chaque émission de la clé.

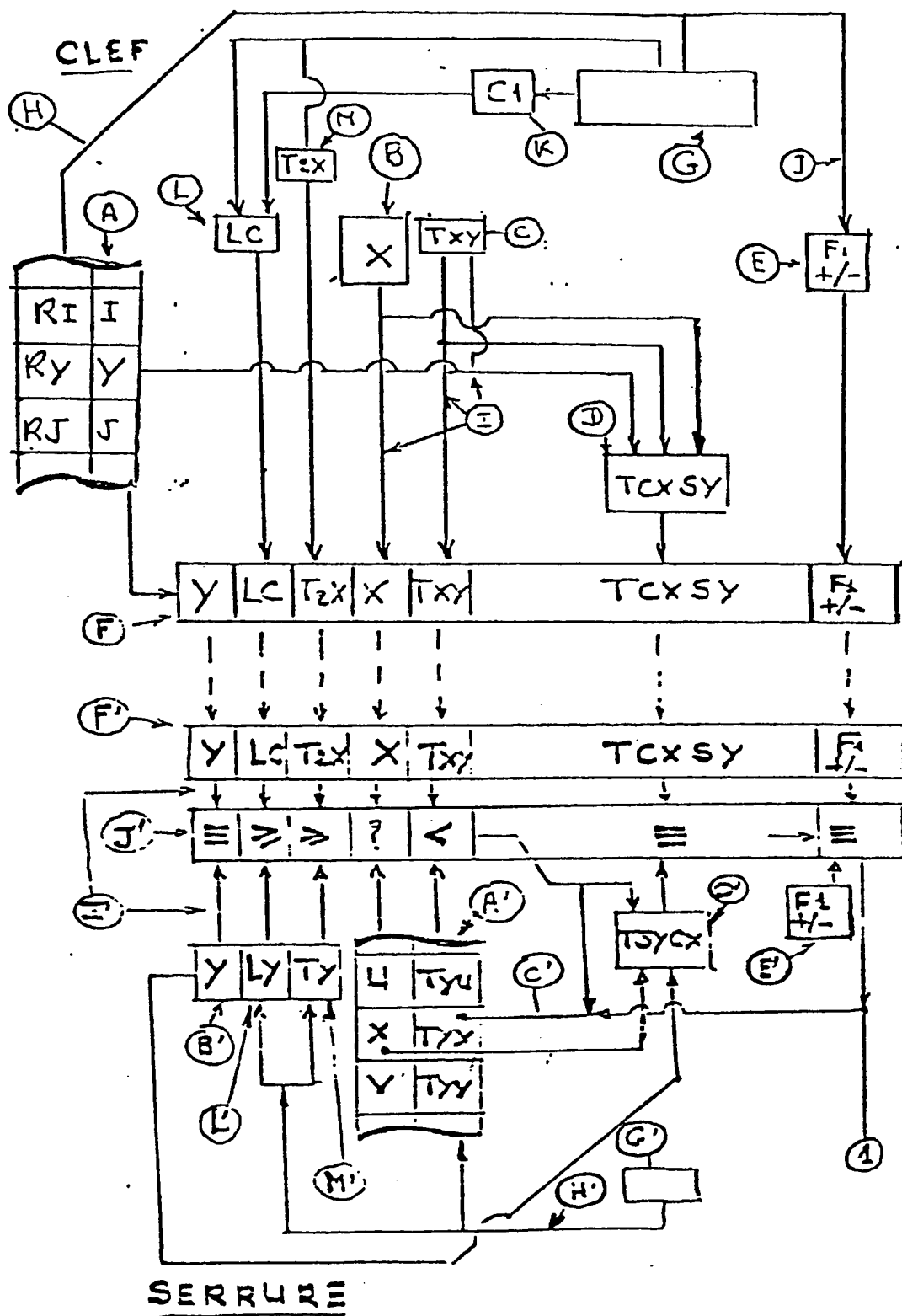
8. Système de clés et serrure selon les revendications 1 à 7 prises dans leur ensemble, caractérisé en ce que la clé comporte une table associant aux numéros des serrures à actionner un repère de cette serrure librement choisi par l'utilisateur de chaque clé.

9. Système de clés et de serrures selon les revendications 1 à 8 prises dans leur ensemble, caractérisé en ce que la clé comporte un comparateur déterminant quelle portion du code d'utilisation de la clé a été introduite dans cette dernière avant la dernière manoeuvre, associé à une horloge déterminant depuis quel délai cette portion de code a été introduit dans la clé avant la dernière manoeuvre et générant les signaux correspondants émis vers la serrure.

10. Système selon la revendication 9 caractérisé en ce que la serrure comporte une mémoire de la portion minimale de ce code à introduire dans la serrure et une mémoire du temps maximum depuis lequel cette portion de code doit avoir été introduite.

11. Système selon les revendications 9 et 10 caractérisé en ce que la serrure comprend un comparateur déterminant si la longueur minimale du code d'utilisation de la clé est bien égal ou supérieur à la longueur minimale imposée par la serrure d'une part, et déterminant si le délai depuis lequel cette portion de code a été introduite dans la clé est inférieur au délai

maximum imposé par la serrure, d'autre part, autorisant ainsi ou interdisant la manoeuvre de la serrure, les dites comparaisons s'effectuant sur les signaux émis par les clés et reçus par les serrures, la fonction anti-fraude sur les clés étant incorporée dans la serrure.





Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 87 45 0009

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.4)
Y	WO-A-8 501 980 (UNIVERSAL PHOTONICS) * Figures 1-2; page 10, ligne 20 - page 15, ligne 31 *	1	E 05 B 49/00
A	---	2, 6	
Y	EP-A-0 043 270 (OMRON TATEISI ELECTRONICS) * Figures 2, 6, 9; page 9, ligne 16 - page 11, ligne 9; page 12, ligne 1 - page 14, ligne 24; page 22, ligne 22 - page 31, ligne 24 *	1	
A	---	2, 3, 7	
Y	FR-A-2 536 781 (KIEKERT GmbH) * Figures; page 1, lignes 10-15; page 3, ligne 1 - page 4, ligne 23 *	1	DOMAINES TECHNIQUES RECHERCHES (Int. Cl.4) E 05 B G 07 C G 07 F
A	---	2, 3, 5, 6	
A	EP-A-0 098 437 (STELLBERGER) * Figures 1-3; page 9, ligne 15 - page 20, ligne 16 *	1-7	
	---	-/-	
Le présent rapport de recherche a été établi pour toutes les revendications			
Lieu de la recherche LA HAYE		Date d'achèvement de la recherche 13-07-1987	Examineur HERBELET J.C.
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

0244332



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande

EP 87 45 0009

Page 2

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl. 4)
A	EP-A-O 099 762 (LEWINER, HENNION) -----	1	
			DOMAINES TECHNIQUES RECHERCHES (Int. Cl. 4)
Le présent rapport de recherche a été établi pour toutes les revendications			
Lieu de la recherche LA HAYE		Date d'achèvement de la recherche 13-07-1987	Examineur HERBELET J.C.
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>			